Evaluasi Performa *Bitcoin Mining* terhadap Serangan *Selfish Mining* dan *Double Spending*

Tugas Akhir

Sebagai Persyaratan Guna Meraih Gelar Sarjana
Informatika Universitas Muhammadiyah Malang

Daniel Vernandes
201310370311190

Bidang Minat Jaringan

PROGRAM STUDI INFORMATIKA
FAKULTAS TEKNIK
UNIVERSITAS MUHAMMADIYAH MALANG
2019

LEMBAR PERSETUJUAN

Evaluasi Performa *Bitcoin Mining* terhadap Serangan *Selfish Mining* dan *Double Spending*

TUGAS AKHIR

Diajukan Untuk Memenuhi
Persyaratan Guna Meraih Gelar Sarjana Strata 1
Teknik Informatika Universitas Muhammadiyah Malang

Menyetujui,

Pembimbing 1	Pembimbing 2
Diah Risqiwati, S.T., M.T.	**Denar Regata A., S.Kom., M.Kom.**
NIP. 108.1410.0545	**NIP. 108.1612.0591**

LEMBAR PENGESAHAN

EVALUASI PERFORMA BITCOIN MINING TERHADAP SERANGAN SELFISH MINING DAN DOUBLE SPENDING

Tugas Akhir

Sebagai Persyaratan Guna Meraih Gelar Sarjana Strata 1

Teknik Informatika Universitas Muhammadiyah Malang

Disusun Oleh:

Daniel Vernandes

201310370311190

Tugas Akhir ini telah diuji dan dinyatakan lulus melalui sidang majelis penguji

Pada tanggal 11 Oktober 2019

Menyetujui,

Penguji I	**Penguji II**
Wahyu Andhyka Kusuma, M.Kom.	**Aminudin, S.Kom., M.Cs.**
NIP.108.1410.0543	**NIP.108.1703.0594**

Mengetahui,

Ketua Jurusan Teknik Informatika

Gita Indah Marthasari, ST., M.Kom.

NIP. 108.0611.0442

LEMBAR PERNYATAAN

Yang bertanda tangan di bawah ini:

Nama	: Daniel Vernandes
Tempat/Tanggal Lahir	: Madiun, 12 September 1994
NIM	: 201310370311190
Fakultas/Jurusan	: Teknik / Teknik Informatika

Dengan ini saya menyatakan bahwa Tugas Akhir dengan judul **"Evaluasi Performa *Bitcoin Mining* terhadap Serangan *Selfish Mining* dan *Double Spending*"** beserta seluruh isinya adalah karya saya sendiri dan bukan merupakan karya tulis orang lain, baik sebagaian maupun keseluruhan, kecuali dalam bentuk kutipan yang telah disebutkan sumbernya.

Demikisan surat pernyataan ini saya buat dengan sebenar-benarnya. Apabila kemudian ditemukan adanya pelanggaran terhadap etika keilmuan dalam karya saya ini, atau ada klaim dari pihak lain terhadap keaslian karya saya ini maka saya siap menanggung segala bentuk resiko/sanksi yang berlaku.

Malang, 6 Oktober 2019

Yang Membuat Pernyataan

Daniel Vernandes

Dosen Pembimbing I	Dosen Pembimbing II
Diah Risqiwati, S.T., M.T.	**Denar Regata A., S.Kom., M.Kom.**
NIP. 108.1410.0545	**NIP. 108.1612.0591**

KATA PENGANTAR

Dengan memanjatkan puji dan syukur kehadirat Allah SWT yang telah melimpahkan rahmat dan hidayah-Nya, tak lupa shalawat dan salam kepada junjungan Nabi Besar Muhammad SAW, sehingga peneliti dapat menyelesaikan tugas akhir yang berjudul "**Evaluasi Performa Bitcoin Mining Terhadap Serangan Selfish Mining Dan Double Spending**" . Di dalam tulisan ini disajikan pokok-pokok bahasan yang meliputi tempat wisata daerah Madura serta rekomendasi untuk mendapatkan tempat wisata yang sesuai dengan user. Dengan menggunakan algoritma *item based collaborative filtering* untuk penentuan kemiripan, perhitungan prediksi serta uji akurasinya.

Peneliti menyadari sepenuhnya bahwa dalam penulisan tugas akhir ini masih banyak kekurangan dan keterbatasan. Oleh karena itu peneliti mengharapkan saran yang membangun agar tulisan ini bermanfaat bagi perkembangan ilmu pengetahuan.

Malang, 6 Oktober 2019

Daniel Vernandes

DAFTAR ISI

LEMBAR PERSETUJUAN i
LEMBAR PENGESAHAN ii
LEMBAR PERNYATAAN iii
ABSTRAK iv
ABSTRACT v
LEMBAR PERSEMBAHAN 6
KATA PENGANTAR vii
DAFTAR ISI viii
DAFTAR GAMBAR x
DAFTAR TABEL xi
BAB I 1
PENDAHULUAN 1
1.1 Latar Belakang 1
1.2 Rumusan Masalah 3
1.3 Tujuan Penelitian 3
1.4 Cakupan Masalah 3
BAB II 4
LANDASAN TERORI 4
2.1 Tinjauan Pustaka 4
2.2 Bitcoin Mining 5
2.3 Selfish Mining 5
2.4 Double Spending 5
2.5 Block 6
2.6 Network Simulator 3 6
2.7 Bitcoin Simulator 6
2.8 Block Receive Time 7
2.9 Block Propagation Time 7
2.10 Block Size 7
2.11 Total Block 8
2.12 Stale Block 8
2.13 Honest Mining Income 8

2.14 Attacker Income 8

BAB III 10
METODOLOGI PENELITIAN....10
3.1 Alur Penelitian....10
3.2 Studi Literatur 11
3.3 Analisis Kebutuhan 12
3.1.1 Kebutuhan Fungsional 12
3.1.2 Kebutuhan Non-Fungsional 13
3.4 Perancangan Sistem....13
3.5 Mining Process 15
3.5 Skenario & Analisis Pengujian 16
3.5.1 Skenario Serangan *Selfish Mining* 16
3.5.2 Skenario Serangan *Double Spending* 17
BAB IV 19
IMPLEMENTASI DAN PENGUJIAN DAN HASIL....19
4.1 Implementasi Sistem 19
4.1.1 Data Sumber....19
4.1.2 Data Implementasi Pengujian 28
4.1.3 Model Matematis Parameter 30
4.2 Pengujian dan Hasil....33
4.2.1 Pengujian dan Hasil Sebelum Serangan 34
4.2.2 Pengujian dan Hasil Setelah Serangan....34
4.3 Analisis dan Pembahasan 36
4.3.1 Perbandingan Sebelum dan Sesudah Serangan....36
4.3.2 Perbandingan Dampak dari *Selfish Mining* dan *Double Spending* 44
4.3.3 Analisis Hasil Pengujian 52
BAB V 58
KESIMPULAN DAN SARAN....58
5.1 Kesimpulan....58
5.2 Saran....58
DAFTAR PUSTAKA 59

DAFTAR GAMBAR

Gambar 3.1 Diagram Alur Model Penelitian 10
Gambar 3.2 Rancangan Sistem 14
Gambar 3.3 Proses Bitcoin Mining 15
Gambar 3.4 Tahap Awal *Selfish Mining*. 16
Gambar 3.5 Injeksi *Selfish Mining* 16
Gambar 3.6 Injeksi *Selfish Mining* 17
Gambar 3.7 Publikasi *Selfish Mining* 17
Gambar 3.8 Publikasi *Selfish Mining* 17
Gambar 3.9 Tahap Awal *Double Spending* 17
Gambar 3.10 Injeksi *Double Spending* 18
Gambar 3.11 Injeksi *Double Spending* 18
Gambar 3.12 Publikasi *Double Spending* 18
Gambar 4.1 Download Bandwidth 20
Gambar 4.2 Upload Bandwidth 20
Gambar 4.3 Download Data Europe 21
Gambar 4.4 Upload Data Europe 22
Gambar 4.5 Download Data Australia 22
Gambar 4.6 Upload Data Australia 23
Gambar 4.7 Download Data North America 24
Gambar 4.8 Upload Data North America 24
Gambar 4.9 Download Data South America 25
Gambar 4.10 Upload Data South America 26
Gambar 4.11 Download Data Asia Pacific 26
Gambar 4.12 Upload Data Asia Pacific 27
Gambar 4.13 Download Data Japan 28
Gambar 4.14 Upload Data Japan 28
Gambar 4.15 Kecepatan Node Sebelum Serangan 29
Gambar 4.16 Lokasi Sebelum Serangan 29
Gambar 4.17 Kecepatan Node Pada Saat Serangan 30
Gambar 4.18 Lokasi Saat Serangan 30
Gambar 4.19 Perbandingan *Block Receive Time Selfish Mining* 36
Gambar 4.20 Perbandingan *Block Receive Time Double Spending* 37
Gambar 4.21 Perbandingan *Block Propagation Time Selfish Mining* 38
Gambar 4.22 Perbandingan *Block Propagation Time Double Spending* 38
Gambar 4.23 Perbandingan *Block Size Selfish Mining* 39
Gambar 4.24 Perbandingan *Block Size Double Spending* 40
Gambar 4.25 Perbandingan *Stale Block Selfish Mining* 41
Gambar 4.26 Perbandingan *Stale Block Double Spending* 41
Gambar 4.27 Perbandingan *Total Block Selfish Mining* 42
Gambar 4.28 Perbandingan *Total Block Double Spending* 43
Gambar 4.29 Perbandingan *Block Receive Time* 44
Gambar 4.30 Perbandingan *Block Propagation Time* 45

Gambar 4.31 Perbandingan *Block Size*.....46
Gambar 4.32 Perbandingan *Stale Block*.....47
Gambar 4.33 Perbandingan *Total Block*.....48
Gambar 4.34. Perbandingan *Income Selfish Mining*.....49
Gambar 4.35 Perbandingan *Income Double Spending*.....50
Gambar 4.36 Perbandingan *Income Selfish Mining dan Double Spending*.....51
Gambar 4.37 Perbandingan *Block Receive Time* sebelum dan setelah serangan.....52
Gambar 4.38 Perbandingan *Block Propagation Time* sebelum dan setelah serangan.....53
Gambar 4.39 Perbandingan *Block Size* sebelum dan setelah serangan.....54
Gambar 4.40 Perbandingan *Stale Block* sebelum dan setelah serangan.....55
Gambar 4.41 Perbandingan *Total Block* sebelum dan setelah serangan.....56
Gambar 4.42 Perbandingan *Mining Income* sebelum dan setelah serangan.....57

DAFTAR TABEL

Tabel 3.1 Literatur Pengujian & Perbandingan 11
Tabel 4.1 Hasil Pengujian *Bitcoin Mining* pada 100 *block* 34
Tabel 4.2 Hasil Pengujian *Bitcoin Mining* pada 200 *block* 34
Tabel 4.3 Hasil Pengujian *Bitcoin Mining* pada 300 *block* 34
Tabel 4.4 Hasil Pengujian *Selfish Mining* pada 100 *block* 35
Tabel 4.5 Hasil Pengujian *Selfish Mining* pada 200 *block* 35
Tabel 4.6 Hasil Pengujian *Selfish Mining* pada 300 *block* 35
Tabel 4.7 Hasil Pengujian *Double Spending* pada 100 *block* 35
Tabel 4.8 Hasil Pengujian *Double Spending* pada 200 *block* 36
Tabel 4.9 Hasil Pengujian *Double Spending* pada 300 *block* 36

DAFTAR PUSTAKA

[1] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," *Www.Bitcoin.Org*, p. 9, 2008.

[2] P. C. Mullan and P. C. Mullan, "Bitcoin Mining," *Digital Currency Challenge: Shaping Online Payment Systems through Us Financial Regulations*. pp. 97–101, 2014.

[3] I. Eyal and E. G. Sirer, "Majority is not enough: Bitcoin mining is vulnerable," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2014, vol. 8437, pp. 436–454.

[4] K. Nayak, S. Kumar, A. Miller, and E. Shi, "Stubborn mining: Generalizing selfish mining and combining with an eclipse attack," in *Proceedings - 2016 IEEE European Symposium on Security and Privacy, EURO S and P 2016*, 2016, pp. 305–320.

[5] G. O. Karame, M. Roeschlin, A. Gervais, S. Capkun, E. Androulaki, and S. Čapkun, "Misbehavior in Bitcoin: A Study of Double-Spending and Accountability," *ACM Trans. Inf. Syst. Secur.*, vol. 18, no. 1, p. 2, 2015.

[6] G. O. Karame, E. Androulaki, and S. Capkun, "Two Bitcoins at the Price of One? Double-Spending Attacks on Fast Payments in Bitcoin.," *IACR Cryptol. ePrint*, pp. 1–17, 2012.

[7] A. Sapirshtein, Y. Sompolinsky, and A. Zohar, "Optimal selfish mining strategies in bitcoin," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2017, vol. 9603 LNCS, pp. 515–532.

[8] C. Perez-Sola, S. Delgado-Segura, G. Navarro-Arribas, and J. Herrera-Joancomartí, "Double-spending Prevention for Bitcoin zero-confirmation transactions," *Https://Eprint.Iacr.Org/*, 2017.

[9] M. Betancourt, "Bitcoin," *Ctheory*, vol. 0, no. 0, pp. 6–18, 2013.

[10] G. F. Riley and T. R. Henderson, "The ns-3 network simulator," in *Modeling and Tools for Network Simulation*, 2010, pp. 15–34.

UNIVERSITAS MUHAMMADIYAH MALANG
FAKULTAS TEKNIK
PROGRAM STUDI TEKNIK INFORMATIKA
Jl. Raya Tlogomas 246 Malang 65144 Telp. 0341 - 464318 Ext. 247, Fax. 0341 - 460782

FORM CEK PLAGIARISME LAPORAN TUGAS AKHIR

Nama Mahasiswa : Daniel Vernandes

NIM : 201310370311190

Judul TA : Evaluasi Performa *Bitcoin Mining* Terhadap Serangan *Selfish Mining* dan *Double Spending*

Hasil Cek Plagiarisme dengan Turnitin

No.	Komponen Pengecekan	Nilai Maksimal Plagiarisme (%)	Hasil Cek Plagiarisme (%) *
1.	Bab 1 – Pendahuluan	10 %	10 %
2.	Bab 2 – Daftar Pustaka	25 %	7 %
3.	Bab 3 – Analisis dan Perancangan	25 %	20 %
4.	Bab 4 – Implementasi dan Pengujian	15 %	0 %
5.	Bab 5 – Kesimpulan dan Saran	5 %	4 %
6.	Makalah Tugas Akhir	20%	0 %

Mengetahui,

Dosen Pembimbing

Denar Regata Akbi, S.Kom., M.Kom.

NIP. 108.1612.0591

*) Hasil cek plagiarism bisa diisikkan oleh salah satu pembimbing